CLAIMS

1. A padding application method for applying a padding scheme that ensures the security of cryptosystems not using random numbers to cryptosystems in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, the method comprising the steps of:

converting input information into a bit string with a prescribed length or less according to the padding scheme;

converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule; and

supplying an encryption function with the first bit string as data input and the second bit string as random number input;

wherein the prescribed conversion rule is a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings, and satisfies the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function.

2. The padding application method claimed in claim 1, wherein the conversion rule is a rule to divide the bit string into two parts in such a manner as to set the first half of the bit string as the first bit string and the second half of the bit string as the second bit string.

3. The padding application method claimed in claim 1 or 2, wherein the OAEP + padding is employed as the padding scheme, and the NTRU cryptosystem is employed as the cryptosystem using random numbers.

4. A padder used in a padding application method for applying a padding scheme that ensures the security of cryptosystems not using random numbers to cryptosystems in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, the padder comprising:

a conversion means for converting input information into a bit string with a prescribed length or less according to the padding scheme;

a bit string conversion means for converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule; and

an encryption means for supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a ciphertext;

wherein the prescribed conversion rule is a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings, and satisfies the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function.

5. The padder claimed in claim 4, wherein the conversion rule is a rule to divide the bit string into two parts in such a manner as to set the first half of the bit string as the first bit string and the second half of the bit string as the second bit string.

6. The padder claimed in claim 4 or 5, wherein the OAEP + padding is employed as the padding scheme, and the NTRU cryptosystem is employed as the cryptosystem using random numbers.

7. An encryptor for creating a ciphertext by applying a padding

scheme that ensures the security of cryptosystems not using random numbers to a cryptosystem in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, the encryptor comprising:

a padding conversion means for converting an input plaintext into a bit string with a prescribed length or less according to the padding scheme;

a bit string conversion means for converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule; and

an encryption means for supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a ciphertext;

wherein the prescribed conversion rule is a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings, and satisfies the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function.

8. An encryptor for creating a ciphertext by applying a padding scheme that ensures the security of cryptosystems not using random numbers to a cryptosystem in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, the encryptor comprising:

a first encryption means for randomly selecting a private key encryption key, and performs private key encryption for an input plaintext using the private key encryption key to create a first ciphertext;

a padding conversion means for converting the private key encryption key into a bit string with a prescribed length or less according to

the padding scheme;

a bit string conversion means for converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule;

a second encryption means for supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a second ciphertext; and

a ciphertext output means for outputting the first ciphertext and the second ciphertext as a ciphertext;

wherein the prescribed conversion rule is a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings, and satisfies the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function.

9. The encryptor claimed in claim 7 or 8, wherein the conversion rule is a rule to divide the bit string into two parts in such a manner as to set the first half of the bit string as the first bit string and the second half of the bit string as the second bit string.

10. The encryptor claimed in claim 7 or 8, wherein the OAEP + padding is employed as the padding scheme, and the NTRU cryptosystem is employed as the cryptosystem using random numbers.

11. An encryption method for creating a ciphertext by applying a padding scheme that ensures the security of cryptosystems not using random numbers to a cryptosystem in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, the method comprising the steps of:

converting an input plaintext into a bit string with a prescribed

length or less according to the padding scheme;

converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule; and

supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a ciphertext;

wherein the prescribed conversion rule is a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings, and satisfies the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function.

12. An encryption method for creating a ciphertext by applying a padding scheme that ensures the security of cryptosystems not using random numbers to a cryptosystem in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, the method comprising the steps of:

randomly selecting a private key encryption key;

performing private key encryption for an input plaintext using the private key encryption key to create a first ciphertext;

converting the private key encryption key into a bit string with a prescribed length or less according to the padding scheme;

converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule;

supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a second ciphertext; and

outputting the first ciphertext and the second ciphertext as a ciphertext;

wherein the prescribed conversion rule is a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings, and satisfies the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function.

13. The encryption method claimed in claim 11 or 12, wherein the conversion rule is a rule to divide the bit string into two parts in such a manner as to set the first half of the bit string as the first bit string and the second half of the bit string as the second bit string.

14. The encryption method claimed in claim 11 or 12, wherein the OAEP + padding is employed as the padding scheme, and the NTRU cryptosystem is employed as the cryptosystem using random numbers.

15. A decryptor for decrypting a ciphertext created by the encryptor claimed in claim 7, comprising:

a first decryption means for decrypting an input ciphertext to generate a first bit string according to a decryption scheme corresponding to the cryptosystem using random numbers;

a random number recovery means for recovering a random number used for encryption as a second bit string;

a bit string inversion means for inverting the first bit string and the second bit string to a bit string with a prescribed length or less based on the inverse of the conversion rule;

a padding inversion means for removing padding according to the padding scheme from the bit string with a prescribed length or less to retrieve the original plaintext; and

a determination means for verifying the validity of the padding,

and if the padding is valid, outputting the plaintext.

16. A decryptor for decrypting a ciphertext created by the encryptor claimed in claim 8, comprising:

a first decryption means for decrypting the second ciphertext to generate a first bit string according to a decryption scheme corresponding to the cryptosystem using random numbers;

a random number recovery means for recovering a random number used for encryption as a second bit string;

a bit string inversion means for inverting the first bit string and the second bit string to a bit string with a prescribed length or less based on the inverse of the conversion rule;

a padding inversion means for removing padding according to the padding scheme from the bit string with a prescribed length or less to retrieve the original private key encryption key; and

a second decryption means for verifying the validity of the padding, and if the padding is valid, decrypting the first ciphertext using the private key encryption key.

17. A decryption method for decrypting a ciphertext created according to the encryption method claimed in claim 11, comprising the steps of:

decrypting an input ciphertext to generate a first bit string according to a decryption scheme corresponding to the cryptosystem using random numbers;

recovering a random number used for encryption as a second bit string;

inverting the first bit string and the second bit string to a bit string with a prescribed length or less based on the inverse of the conversion rule;

removing padding according to the padding scheme from the bit string with a prescribed length or less to retrieve the original plaintext; and

verifying the validity of the padding, and if the padding is valid, outputting the plaintext.

18. A decryption method for decrypting a ciphertext created according to the encryption method claimed in claim 12, comprising the steps of:

decrypting the second ciphertext to generate a first bit string according to a decryption scheme corresponding to the cryptosystem using random numbers;

recovering a random number used for encryption as a second bit string;

inverting the first bit string and the second bit string to a bit string with a prescribed length or less based on the inverse of the conversion rule;

removing padding according to the padding scheme from the bit string with a prescribed length or less to retrieve the original private key encryption key; and

verifying the validity of the padding, and if the padding is valid, decrypting the first ciphertext using the private key encryption key.

19. A cryptographic communication system comprising communication terminals that perform cryptographic communication through a communication network using a padding scheme that ensures the security of cryptosystems not using random numbers with a cryptosystem in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, wherein:

a sending communication terminal includes:

a padding conversion means for converting an input plaintext

into a bit string with a prescribed length or less according to the padding scheme;

a bit string conversion means for converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule, the conversion rule being a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings and satisfying the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function;

an encryption means for supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a ciphertext; and

a transmission means for transmitting the ciphertext to a receiving terminal; and

the receiving communication terminal includes:

a reception means for receiving the ciphertext from the sending communication terminal;

a first decryption means for decrypting the received ciphertext to generate a first bit string according to a decryption scheme corresponding to the cryptosystem using random numbers;

a random number recovery means for recovering a random number used for the encryption as a second bit string;

a bit string inversion means for inverting the first bit string and the second bit string to a bit string with a prescribed length or less based on the inverse of the conversion rule;

a padding inversion means for removing padding according to the padding scheme from the bit string with a prescribed length or less to retrieve the original plaintext; and

a determination means for verifying the validity of the

padding, and if the padding is valid, outputting the plaintext.

20. A cryptographic communication system comprising communication terminals that perform cryptographic communication through a communication network using a padding scheme that ensures the security of cryptosystems not using random numbers with a cryptosystem in which a random number used to create a ciphertext is susceptible to recovery at the receiving end, wherein:

a sending communication terminal includes:

a first encryption means for randomly selecting a private key encryption key, and performs private key encryption for an input plaintext using the private key encryption key to create a first ciphertext;

a padding conversion means for converting the private key encryption key into a bit string with a prescribed length or less according to the padding scheme;

a bit string conversion means for converting the bit string into a first bit string and a second bit string based on a prescribed conversion rule, the conversion rule being a map to map the bit string having a prescribed length or less to the element of the direct product of the set of the first bit strings and the set of the second bit strings and satisfying the following conditions: the map is injective; the map and inverse map thereof are computable by a polynomial time; and the encryption function whose domain is the direct product is a one-way function;

a second encryption means for supplying an encryption function with the first bit string as data input and the second bit string as random number input to create a second ciphertext; and

a ciphertext output means for outputting the first ciphertext and the second ciphertext as a ciphertext; and

a receiving communication terminal includes:

a reception means for receiving the ciphertext from the

sending communication terminal;

a first decryption means for decrypting the second ciphertext to generate a first bit string according to a decryption scheme corresponding to the cryptosystem using random numbers;

a random number recovery means for recovering a random number used for the encryption as a second bit string;

a bit string inversion means for inverting the first bit string and the second bit string to a bit string with a prescribed length or less based on the inverse of the conversion rule;

a padding inversion means for removing padding according to the padding scheme from the bit string with a prescribed length or less to retrieve the original private key encryption key; and

a second decryption means for verifying the validity of the padding, and if the padding is valid, decrypting the first ciphertext using the private key encryption key.